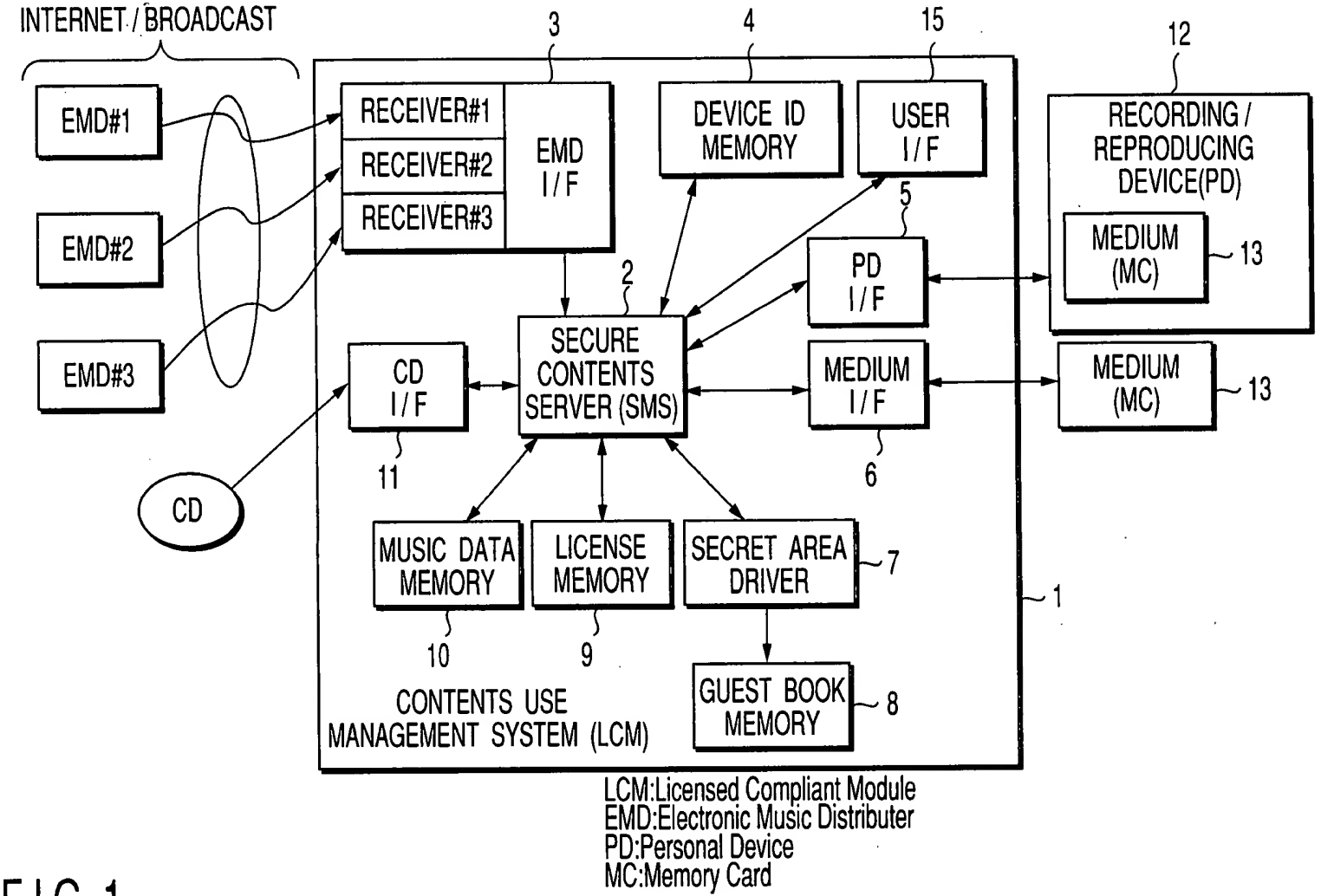
INTERNET / BROADCAST
EMD#1
EMD#2
EMD#3
CD
3
RECEIVER#1
RECEIVER#2
RECEIVER#3
EMD I/F
4
DEVICE ID MEMORY
15
USER I/F
12
RECORDING / REPRODUCING DEVICE(PD)
MEDIUM (MC)
13
5
PD I/F
2
SECURE CONTENTS SERVER (SMS)
CD I/F
11
MEDIUM I/F
6
MEDIUM (MC)
13
MUSIC DATA MEMORY
10
LICENSE MEMORY
9
SECRET AREA DRIVER
7
GUEST BOOK MEMORY
8
1
CONTENTS USE MANAGEMENT SYSTEM (LCM)
LCM:Licensed Compliant Module
EMD:Electronic Music Distributer
PD:Personal Device
MC:Memory Card

FIG. 1

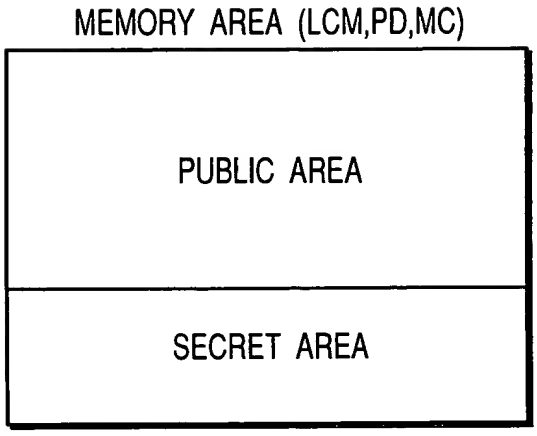
MEMORY AREA (LCM,PD,MC)
PUBLIC AREA
SECRET AREA

FIG. 2

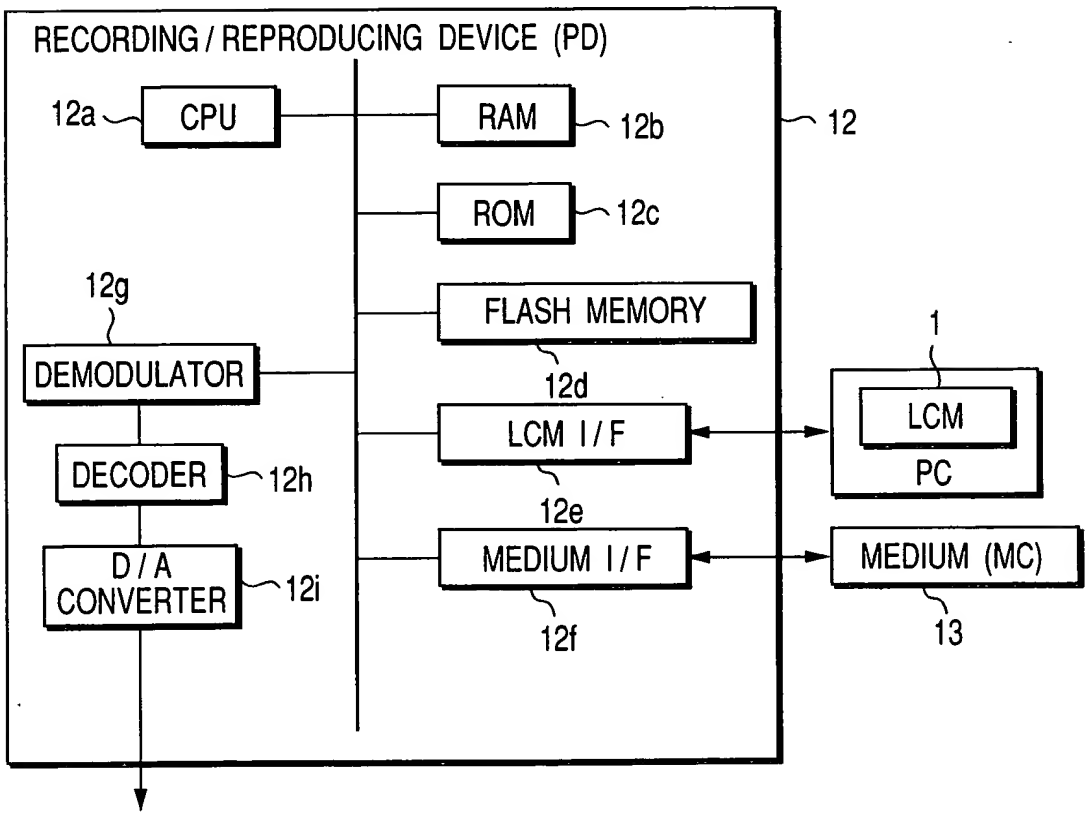
RECORDING / REPRODUCING DEVICE (PD)
12a
CPU
RAM
12b
12
ROM
12c
12g
FLASH MEMORY
1
DEMODULATOR
12d
LCM
LCM I / F
DECODER
12h
PC
12e
D / A CONVERTER
12i
MEDIUM I / F
MEDIUM (MC)
12f
13

FIG. 3

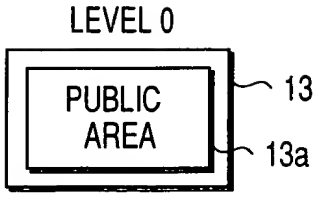

FIG. 4A

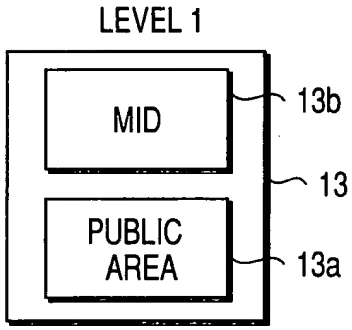

FIG. 4B

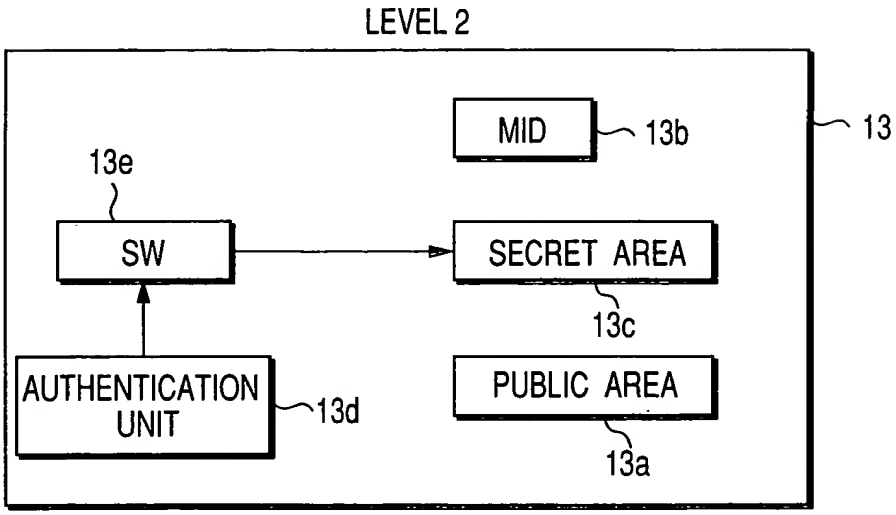

FIG. 4C

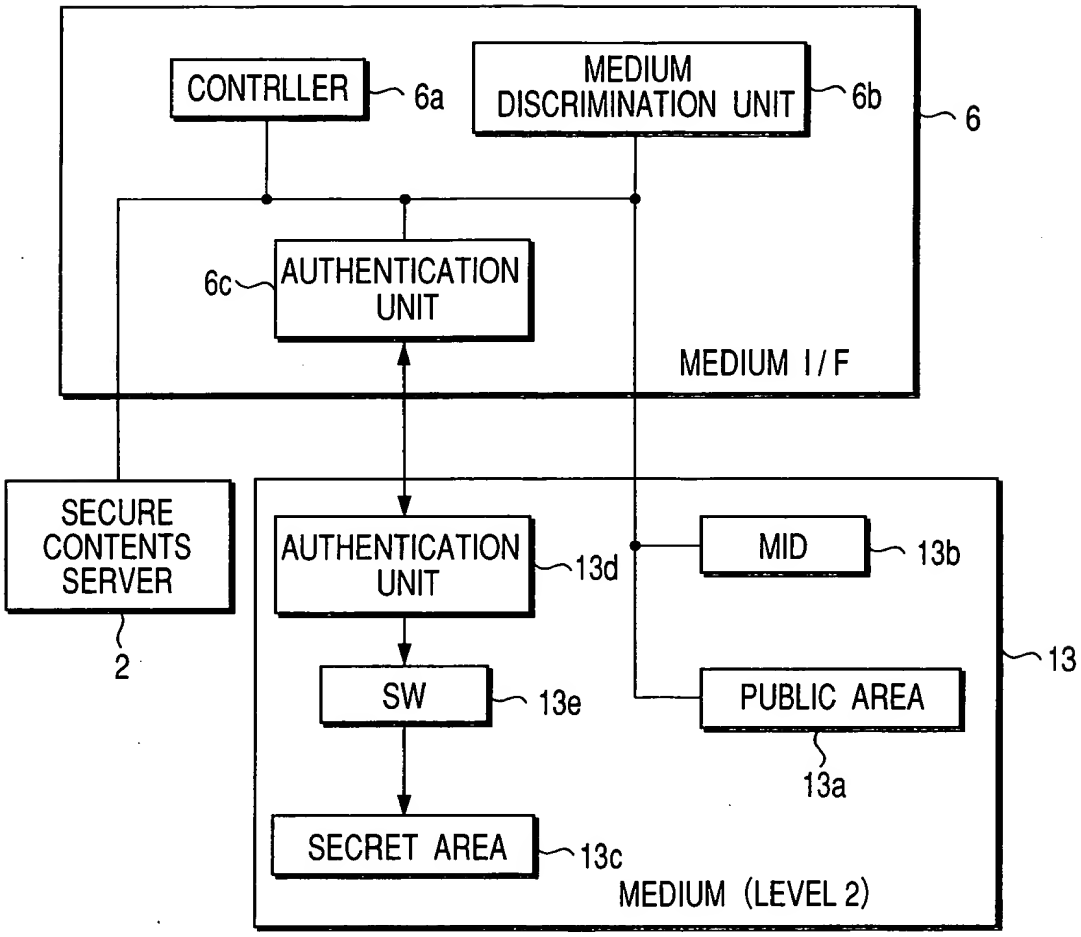
CONTRLLER
6a
MEDIUM DISCRIMINATION UNIT
6b
6
6c
AUTHENTICATION UNIT
MEDIUM I/F
SECURE CONTENTS SERVER
2
AUTHENTICATION UNIT
13d
MID
13b
SW
13e
PUBLIC AREA
13a
13
SECRET AREA
13c
MEDIUM (LEVEL 2)

FIG. 5

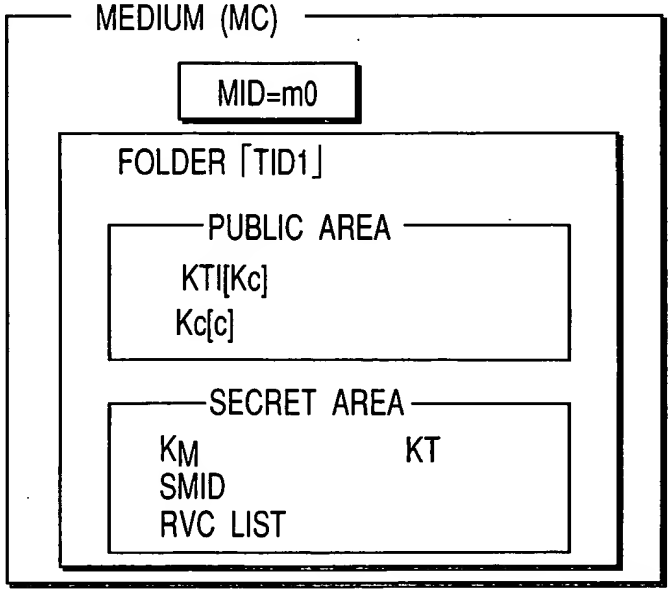
MEDIUM (MC)
MID=m0
FOLDER「TID1」
PUBLIC AREA
KTI[Kc]
Kc[c]
SECRET AREA
K_M
KT
SMID
RVC LIST

FIG. 6

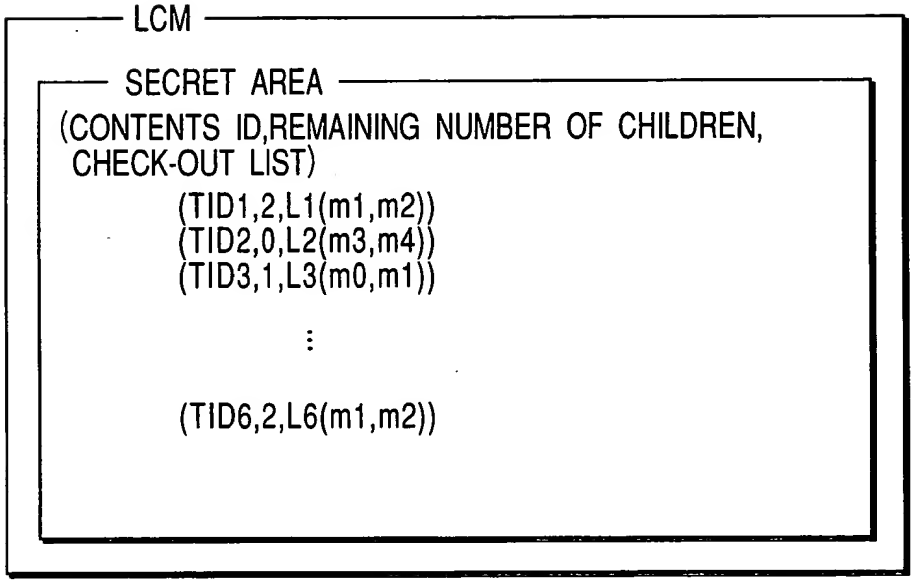

FIG. 7A

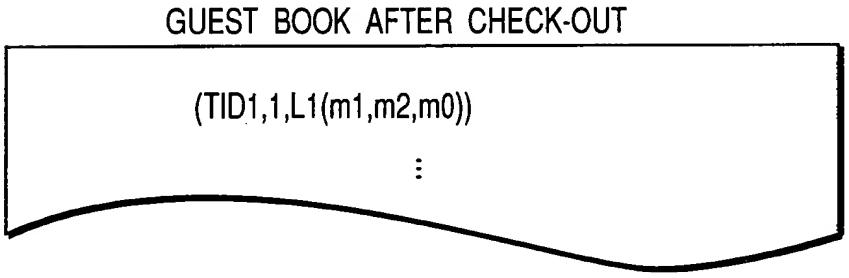

FIG. 7B

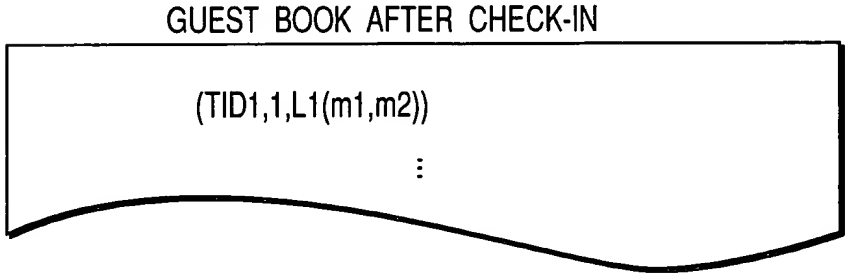

FIG. 7C

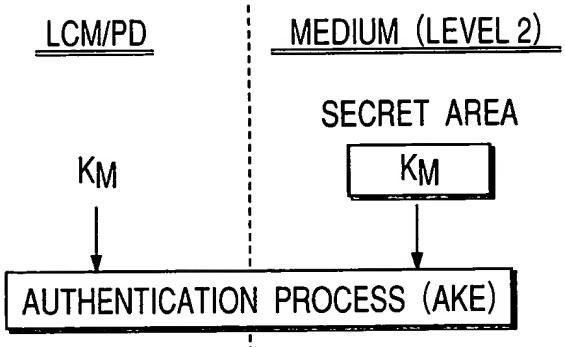

FIG. 8A

KM : GLOBAL SECRET INFORMATION (SECRET INFORMATION COMMON TO GIVEN NUMBER OF MEDIA)

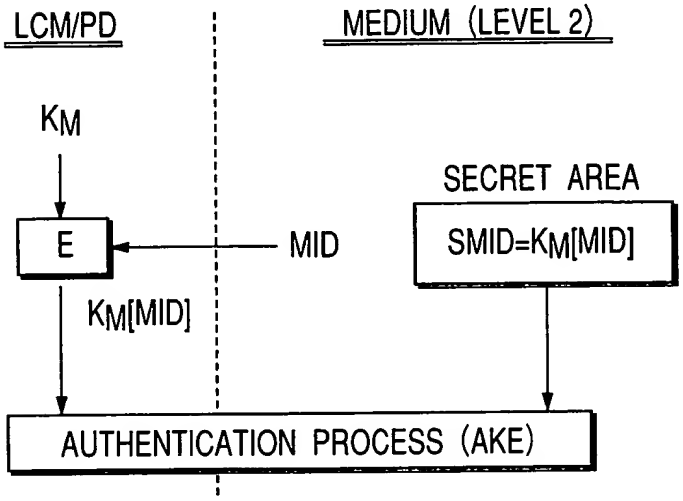

FIG. 8B

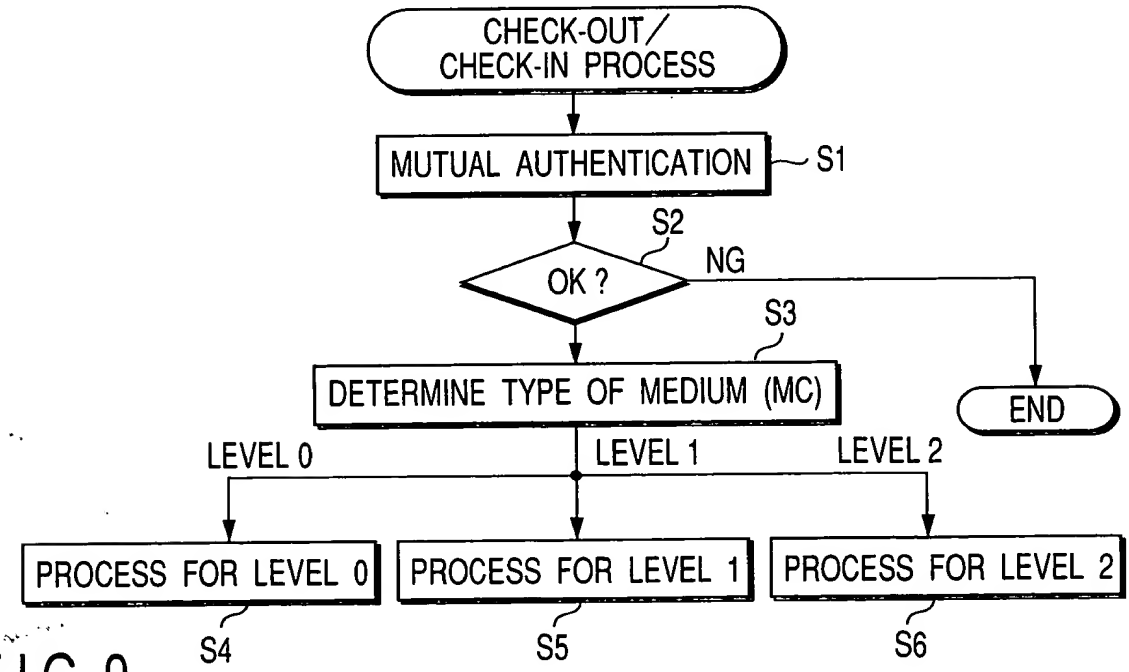

FIG. 9

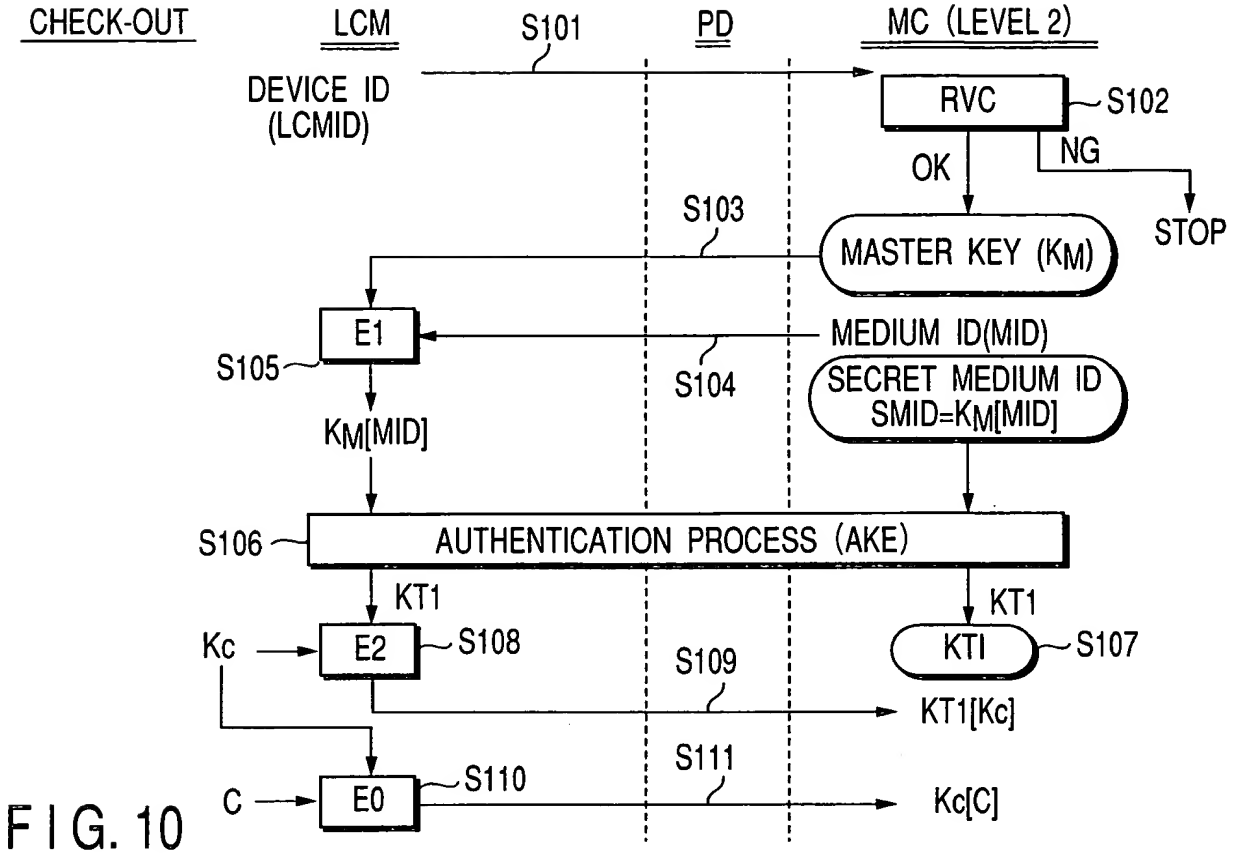
CHECK-OUT
LCM
S101
PD
MC (LEVEL 2)
DEVICE ID
(LCMID)
RVC
S102
NG
OK
STOP
S103
MASTER KEY (KM)
E1
MEDIUM ID(MID)
S105
S104
SECRET MEDIUM ID
SMID=KM[MID]
KM[MID]
S106
AUTHENTICATION PROCESS (AKE)
KT1
KT1
Kc
E2
S108
KTI
S107
S109
KT1[Kc]
S111
C
E0
S110
Kc[C]

FIG. 10

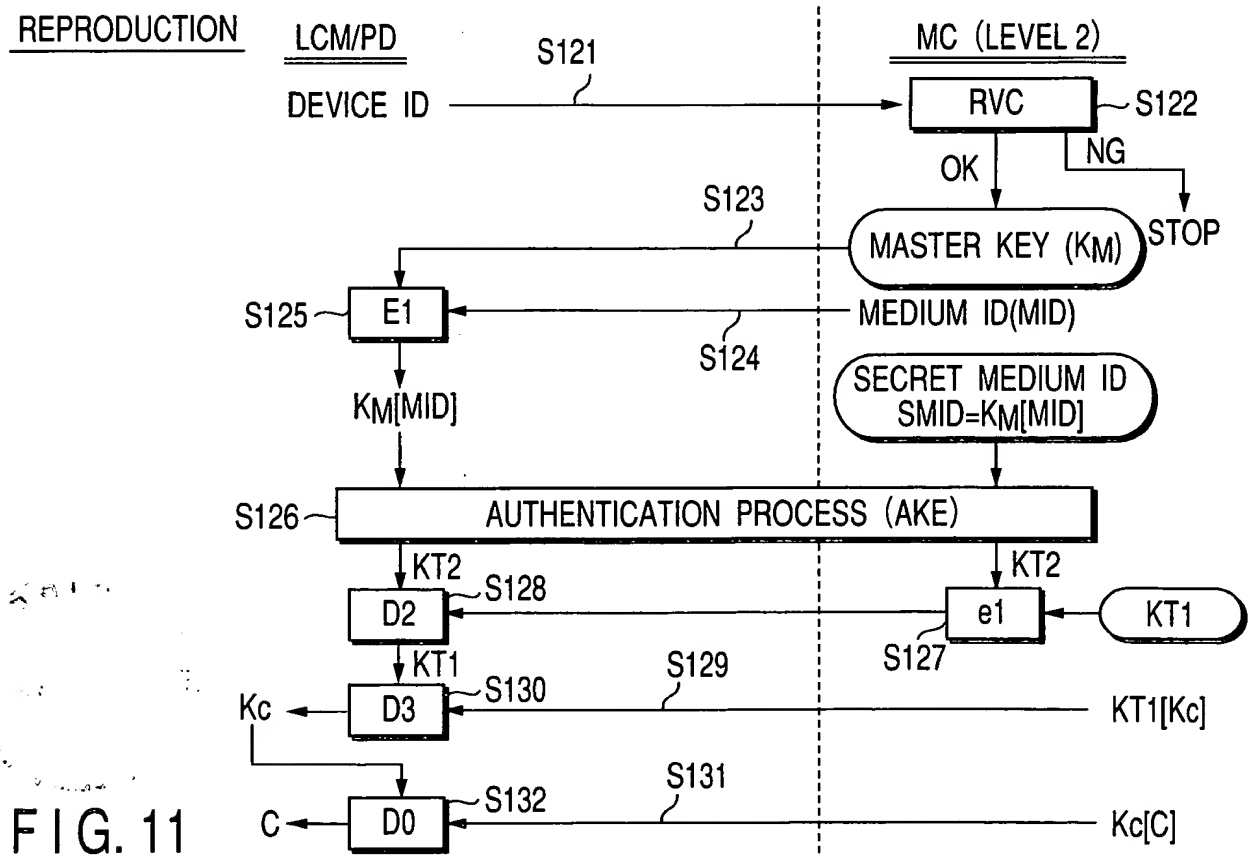
REPRODUCTION
LCM/PD
S121
MC (LEVEL 2)
DEVICE ID
RVC
S122
NG
OK
S123
MASTER KEY (KM)
STOP
S125
E1
MEDIUM ID(MID)
S124
SECRET MEDIUM ID
SMID=KM[MID]
KM[MID]
S126
AUTHENTICATION PROCESS (AKE)
KT2
KT2
D2
S128
e1
KT1
S127
KT1
S129
Kc
D3
S130
KT1[Kc]
S131
C
D0
S132
Kc[C]

FIG. 11

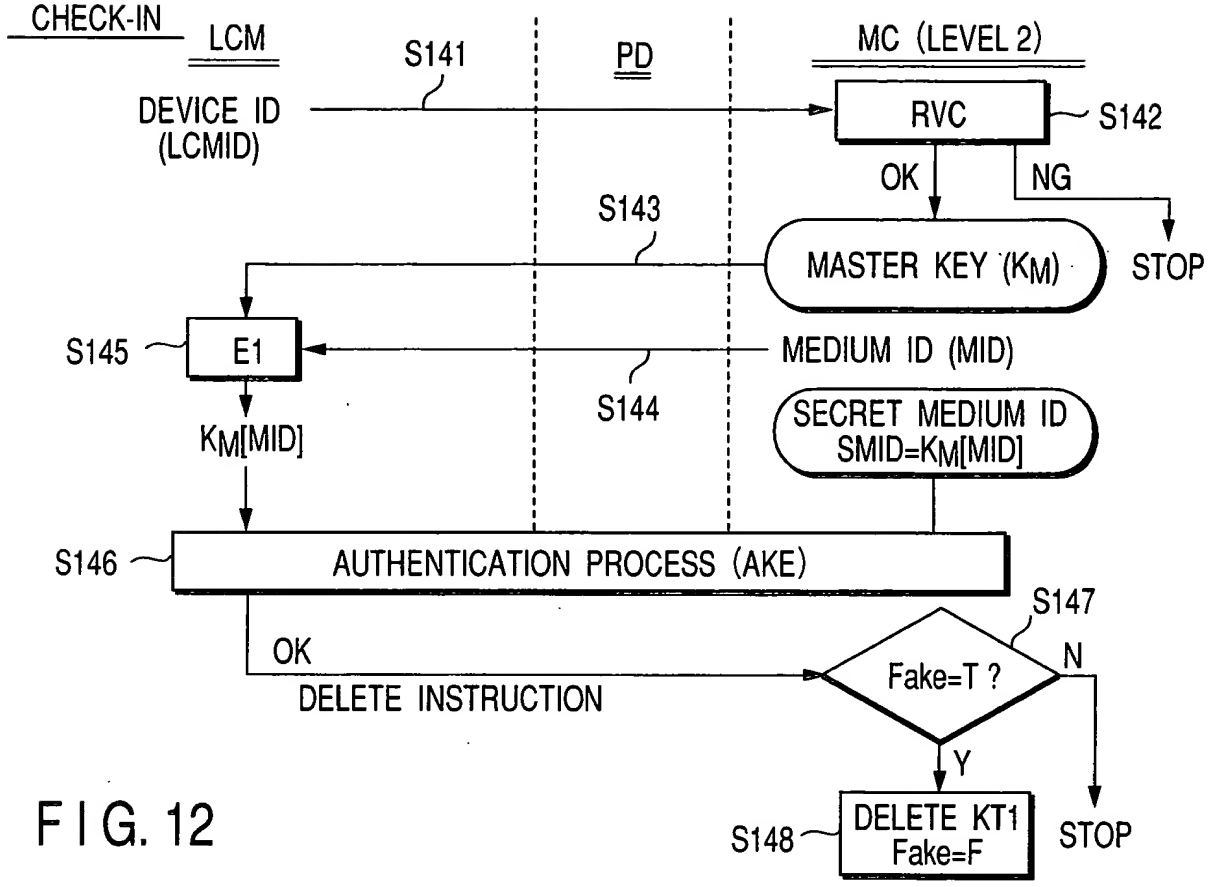
CHECK-IN
LCM
PD
MC (LEVEL 2)
S141
DEVICE ID
(LCMID)
RVC
S142
OK
NG
S143
MASTER KEY (KM)
STOP
S145
E1
MEDIUM ID (MID)
S144
KM[MID]
SECRET MEDIUM ID
SMID=KM[MID]
S146
AUTHENTICATION PROCESS (AKE)
S147
OK
DELETE INSTRUCTION
Fake=T ?
N
Y
S148
DELETE KT1
Fake=F
STOP

FIG. 12

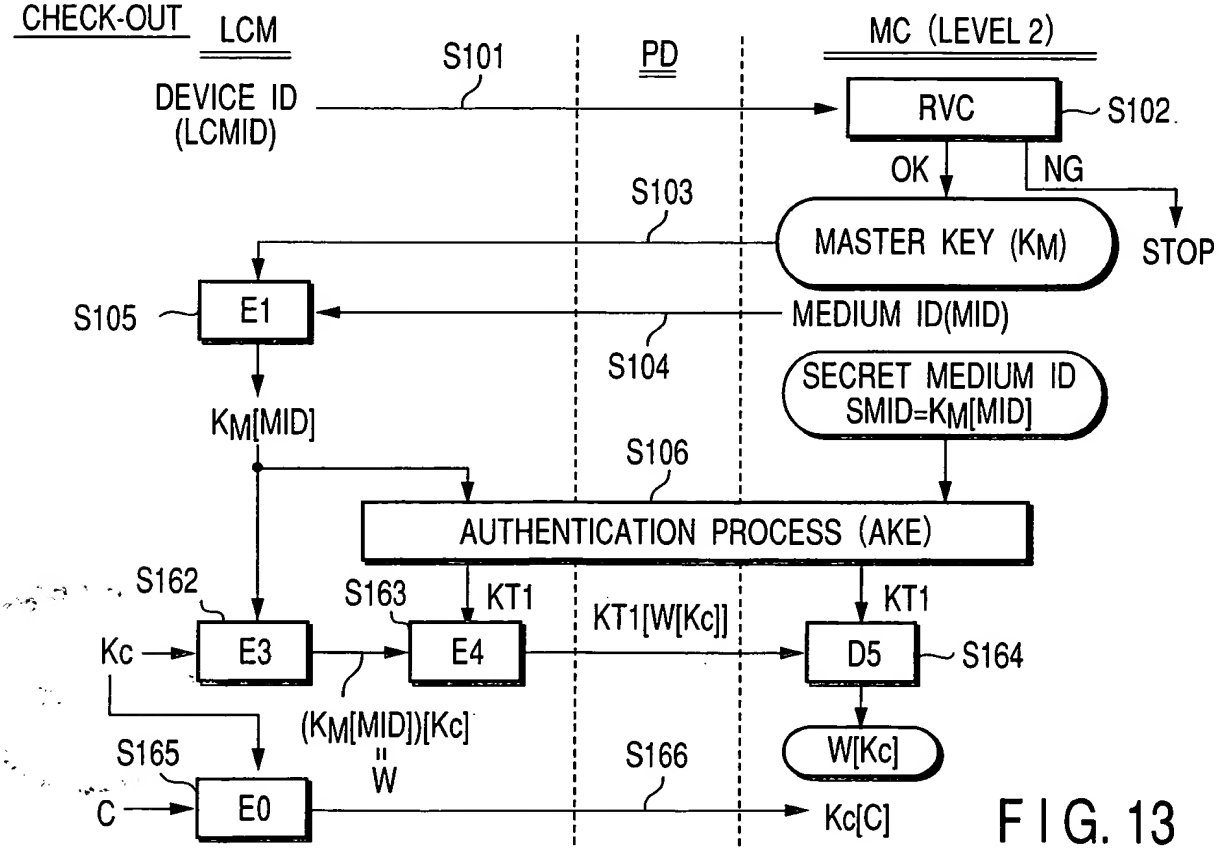
CHECK-OUT
LCM
PD
MC (LEVEL 2)
S101
DEVICE ID
(LCMID)
RVC
S102
OK
NG
S103
MASTER KEY (KM)
STOP
S105
E1
MEDIUM ID(MID)
S104
KM[MID]
SECRET MEDIUM ID
SMID=KM[MID]
S106
AUTHENTICATION PROCESS (AKE)
S162
S163
KT1
KT1[W[Kc]]
KT1
Kc
E3
E4
D5
S164
(KM[MID])[Kc]
=
W
W[Kc]
S165
S166
C
E0
Kc[C]

FIG. 13

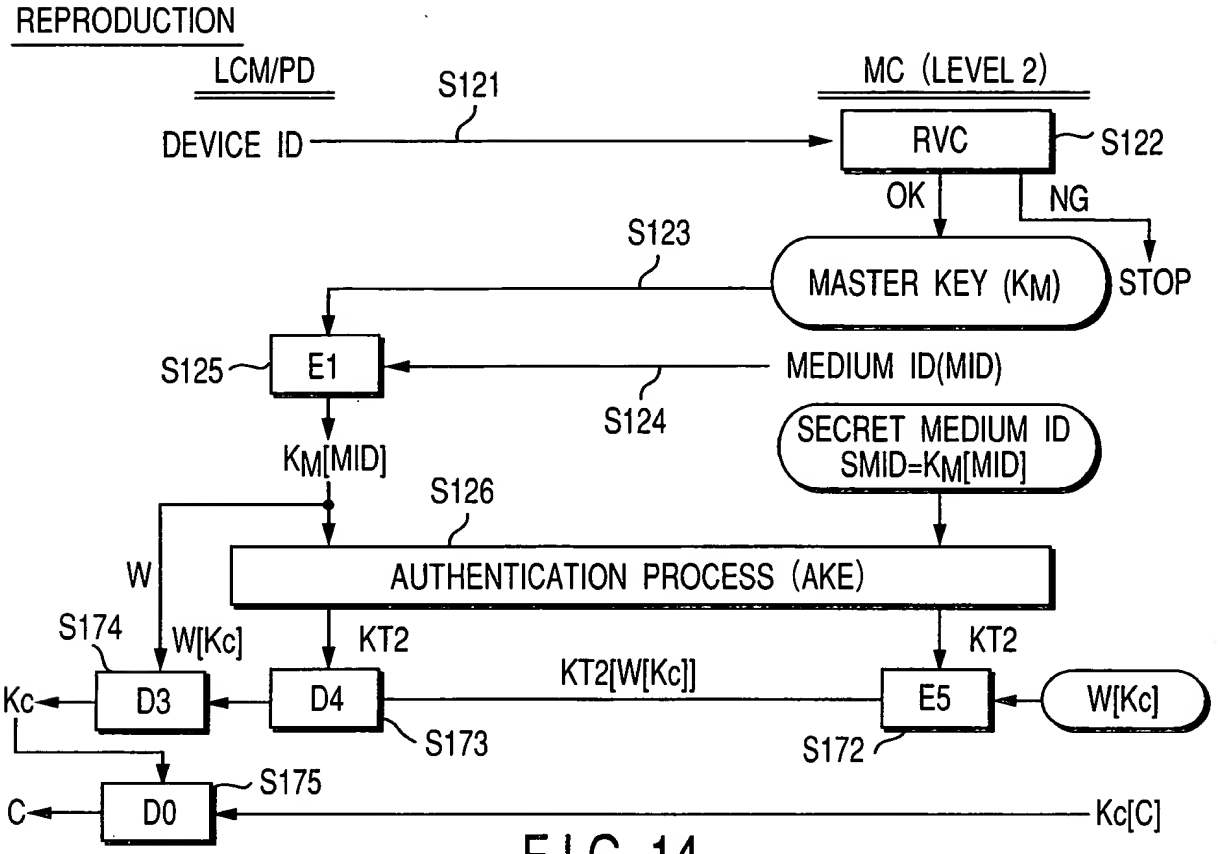
REPRODUCTION
LCM/PD
MC (LEVEL 2)
S121
DEVICE ID
RVC
S122
OK
NG
S123
MASTER KEY (KM)
STOP
S125
E1
MEDIUM ID(MID)
S124
SECRET MEDIUM ID
SMID=KM[MID]
KM[MID]
S126
W
AUTHENTICATION PROCESS (AKE)
S174
W[Kc]
KT2
KT2
KT2[W[Kc]]
Kc
D3
D4
E5
W[Kc]
S173
S172
S175
C
D0
Kc[C]

FIG. 14

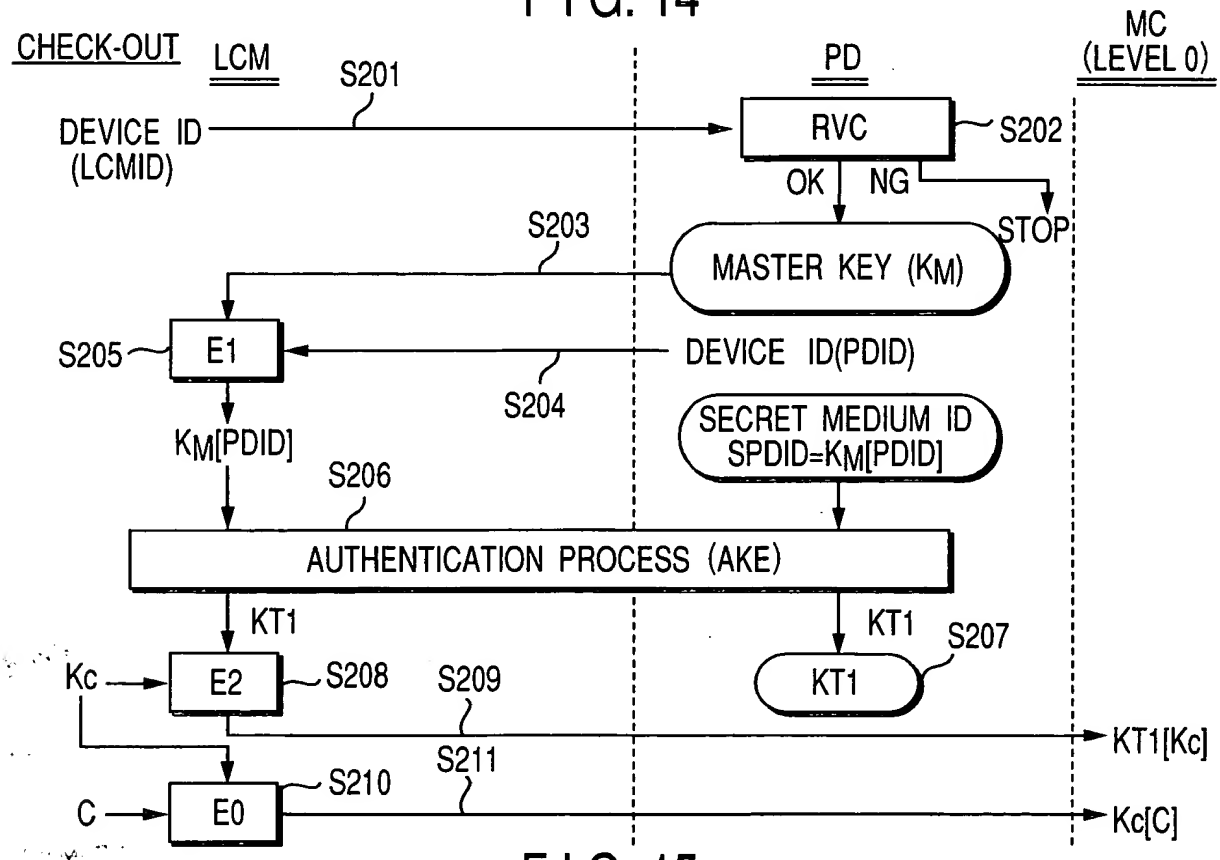
CHECK-OUT
LCM
PD
MC
(LEVEL 0)
S201
DEVICE ID
(LCMID)
RVC
S202
OK
NG
STOP
S203
MASTER KEY (KM)
S205
E1
DEVICE ID(PDID)
S204
SECRET MEDIUM ID
SPDID=KM[PDID]
KM[PDID]
S206
AUTHENTICATION PROCESS (AKE)
KT1
KT1
S207
Kc
E2
S208
S209
KT1
KT1[Kc]
S211
C
E0
S210
Kc[C]

FIG. 15

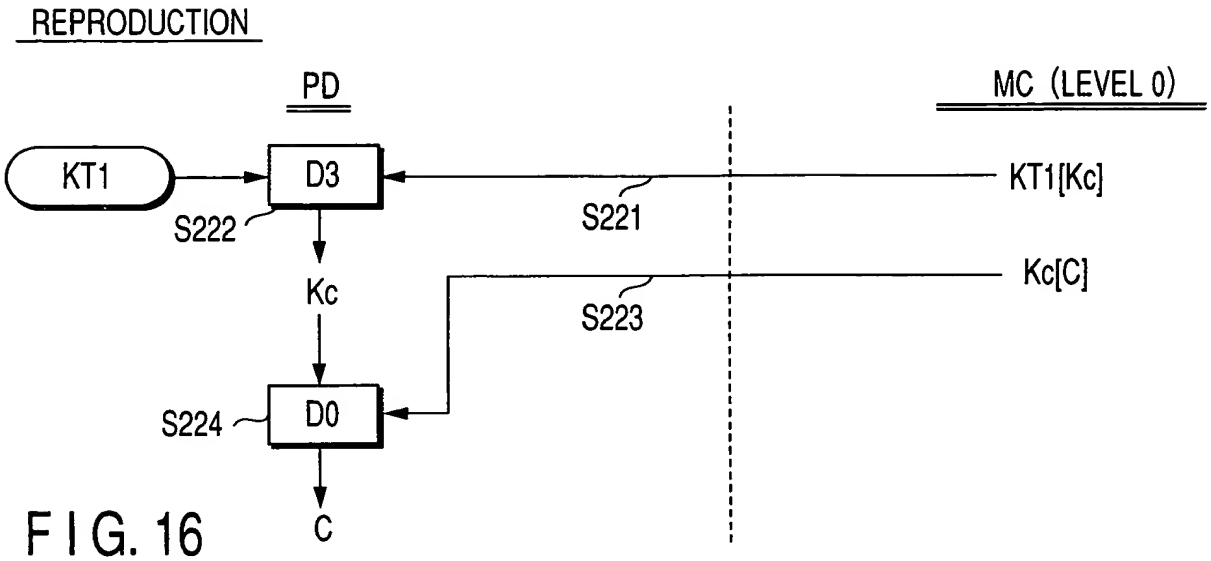
REPRODUCTION
PD
MC (LEVEL 0)
KT1
D3
KT1[Kc]
S222
S221
Kc
Kc[C]
S223
S224
D0
C

FIG. 16

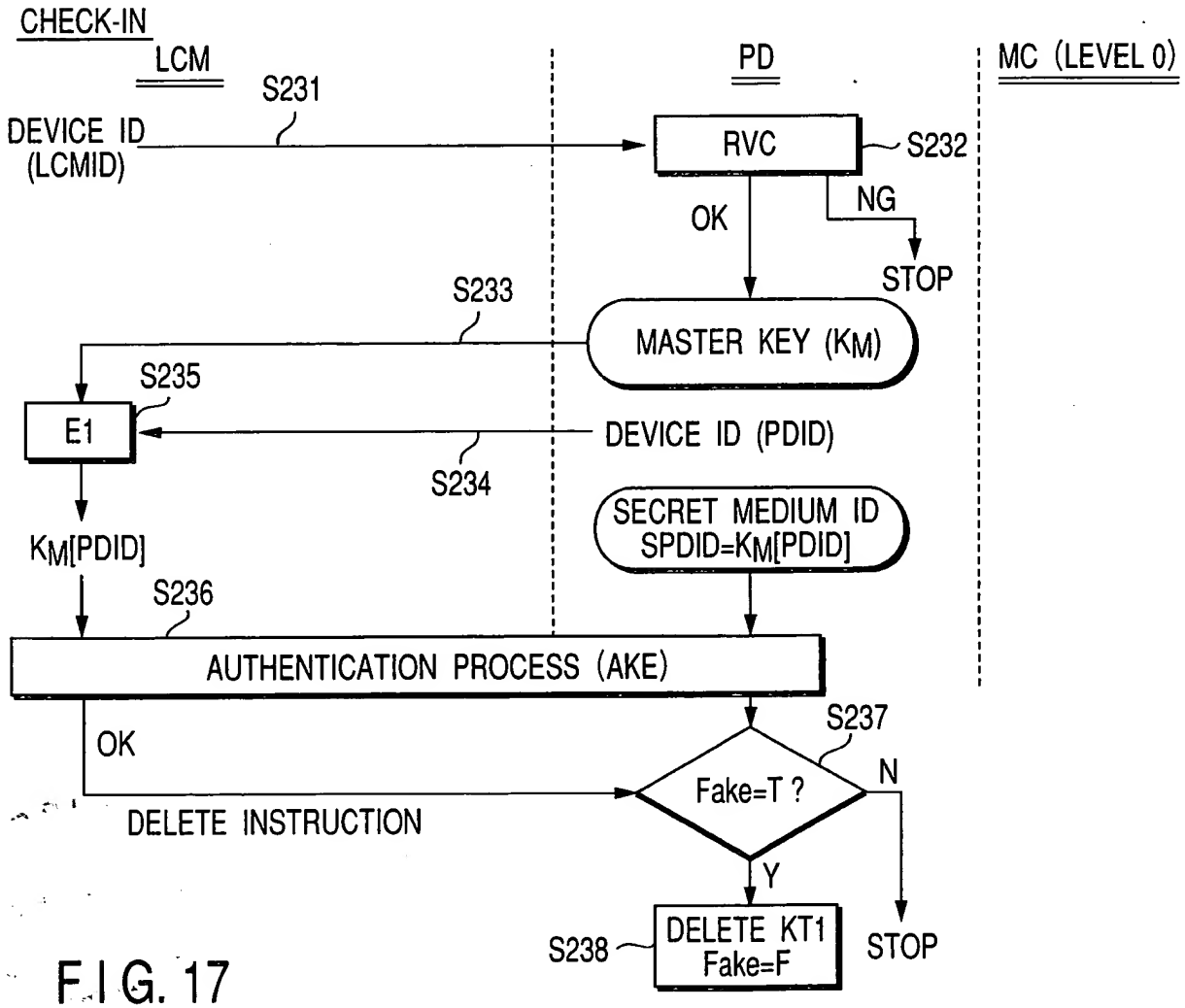
CHECK-IN
LCM
PD
MC (LEVEL 0)
S231
DEVICE ID (LCMID)
RVC
S232
OK
NG
STOP
S233
MASTER KEY (KM)
S235
E1
DEVICE ID (PDID)
S234
SECRET MEDIUM ID SPDID=KM[PDID]
KM[PDID]
S236
AUTHENTICATION PROCESS (AKE)
S237
OK
Fake=T ?
N
DELETE INSTRUCTION
Y
S238
DELETE KT1 Fake=F
STOP

FIG. 17

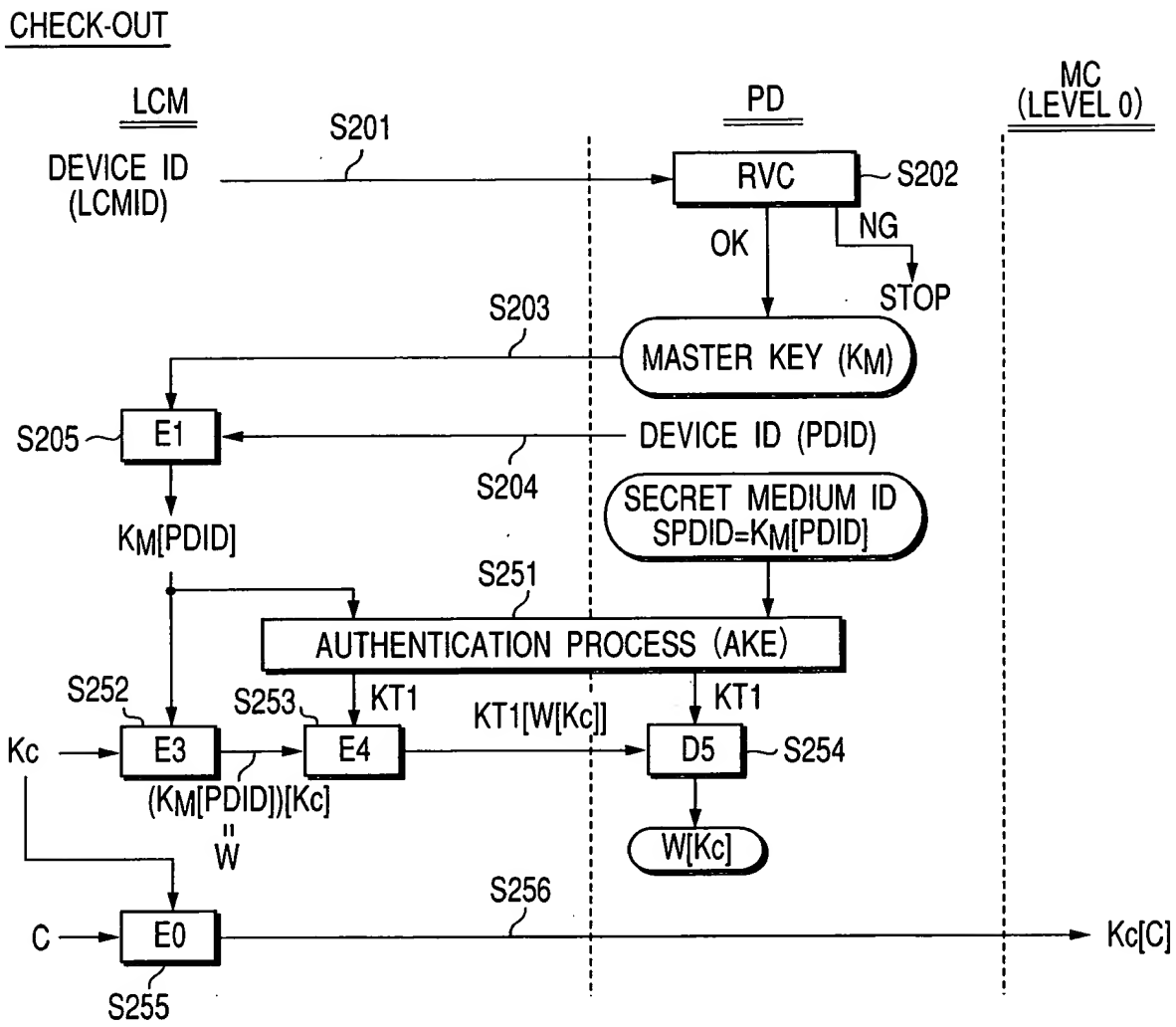
CHECK-OUT
LCM
PD
MC
(LEVEL 0)
S201
DEVICE ID
(LCMID)
RVC
S202
OK
NG
STOP
S203
MASTER KEY (KM)
S205
E1
DEVICE ID (PDID)
S204
KM[PDID]
SECRET MEDIUM ID
SPDID=KM[PDID]
S251
AUTHENTICATION PROCESS (AKE)
S252
S253
KT1
KT1
KT1[W[Kc]]
Kc
E3
E4
D5
S254
(KM[PDID])[Kc]
=
W
W[Kc]
S256
C
E0
Kc[C]
S255

FIG. 18

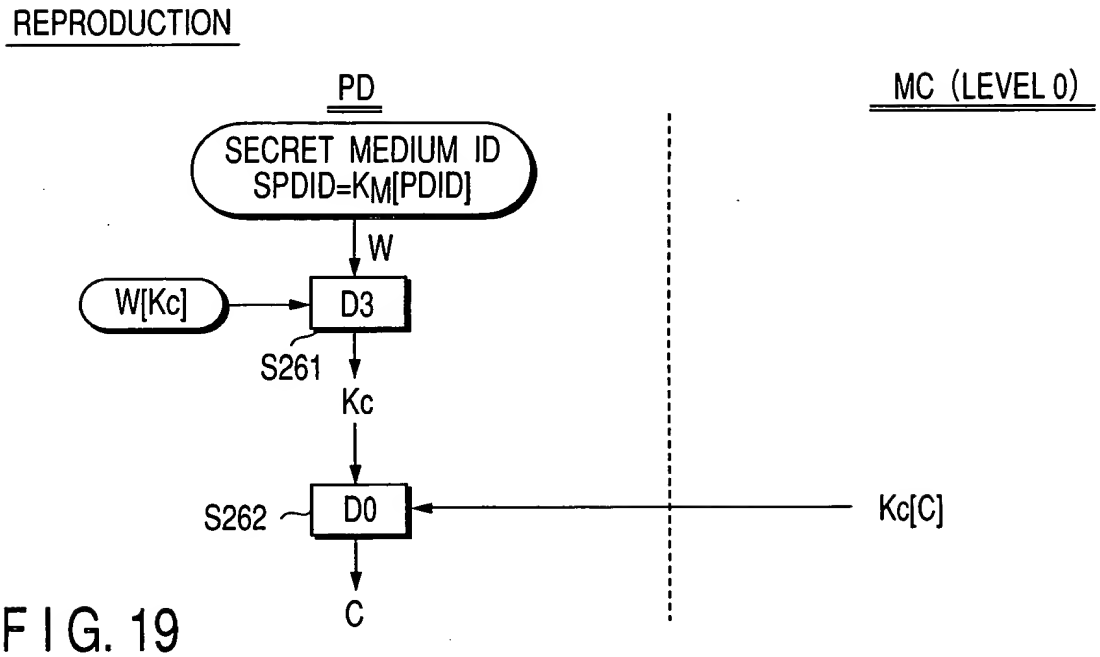
REPRODUCTION
PD
MC (LEVEL 0)
SECRET MEDIUM ID
SPDID=KM[PDID]
W
W[Kc]
D3
S261
Kc
S262
D0
Kc[C]
C

FIG. 19

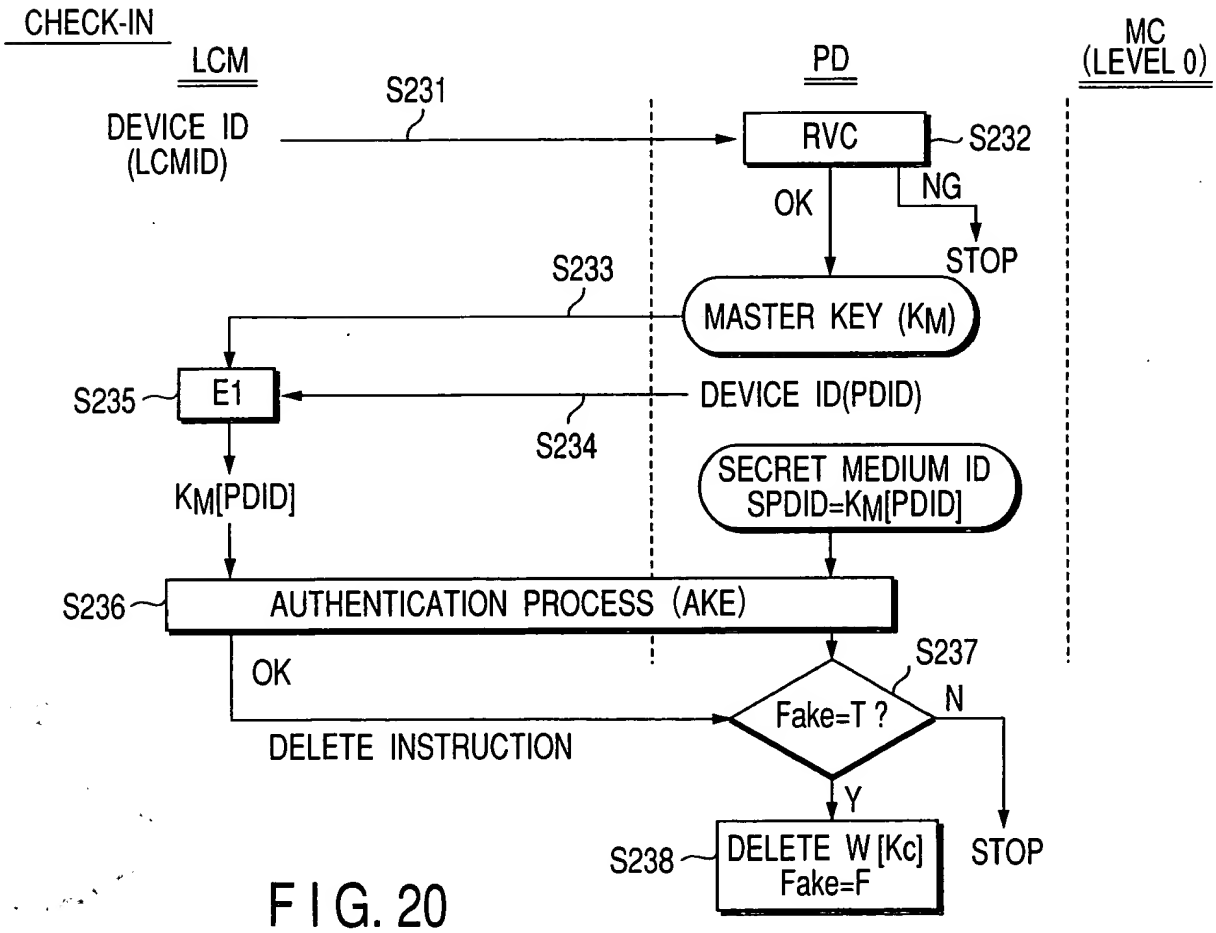
CHECK-IN
LCM
PD
MC
(LEVEL 0)
S231
DEVICE ID
(LCMID)
RVC
S232
OK
NG
STOP
S233
MASTER KEY (KM)
S235
E1
DEVICE ID(PDID)
S234
KM[PDID]
SECRET MEDIUM ID
SPDID=KM[PDID]
S236
AUTHENTICATION PROCESS (AKE)
OK
S237
Fake=T ?
N
DELETE INSTRUCTION
Y
S238
DELETE W [Kc]
Fake=F
STOP

FIG. 20

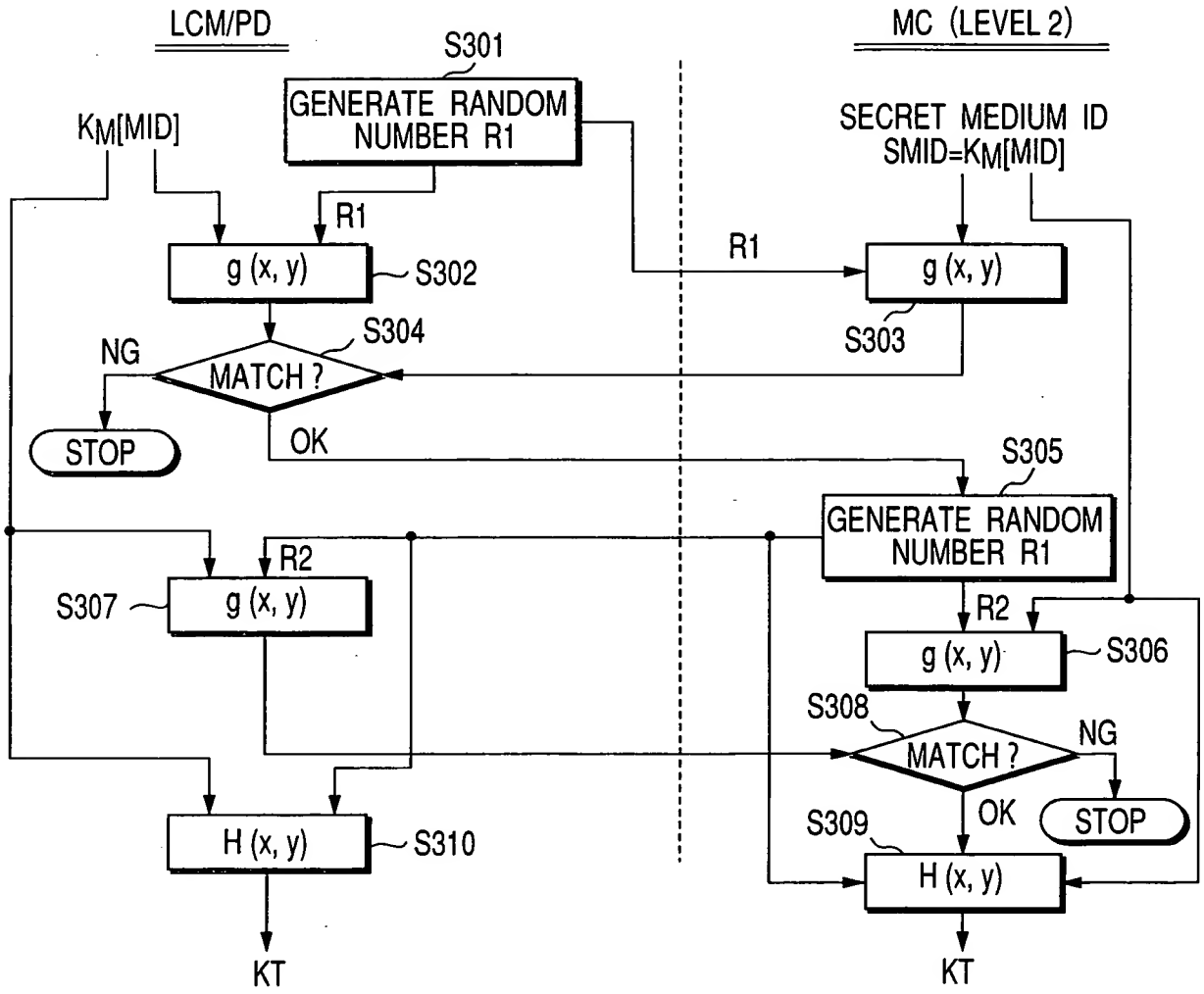
LCM/PD
MC (LEVEL 2)
S301
GENERATE RANDOM NUMBER R1
K_M[MID]
SECRET MEDIUM ID
SMID=K_M[MID]
R1
R1
g (x, y)
S302
g (x, y)
S303
S304
NG
MATCH ?
STOP
OK
S305
GENERATE RANDOM NUMBER R1
R2
S307
g (x, y)
R2
g (x, y)
S306
S308
MATCH ?
NG
OK
STOP
S309
H (x, y)
S310
H (x, y)
KT
KT

FIG. 21

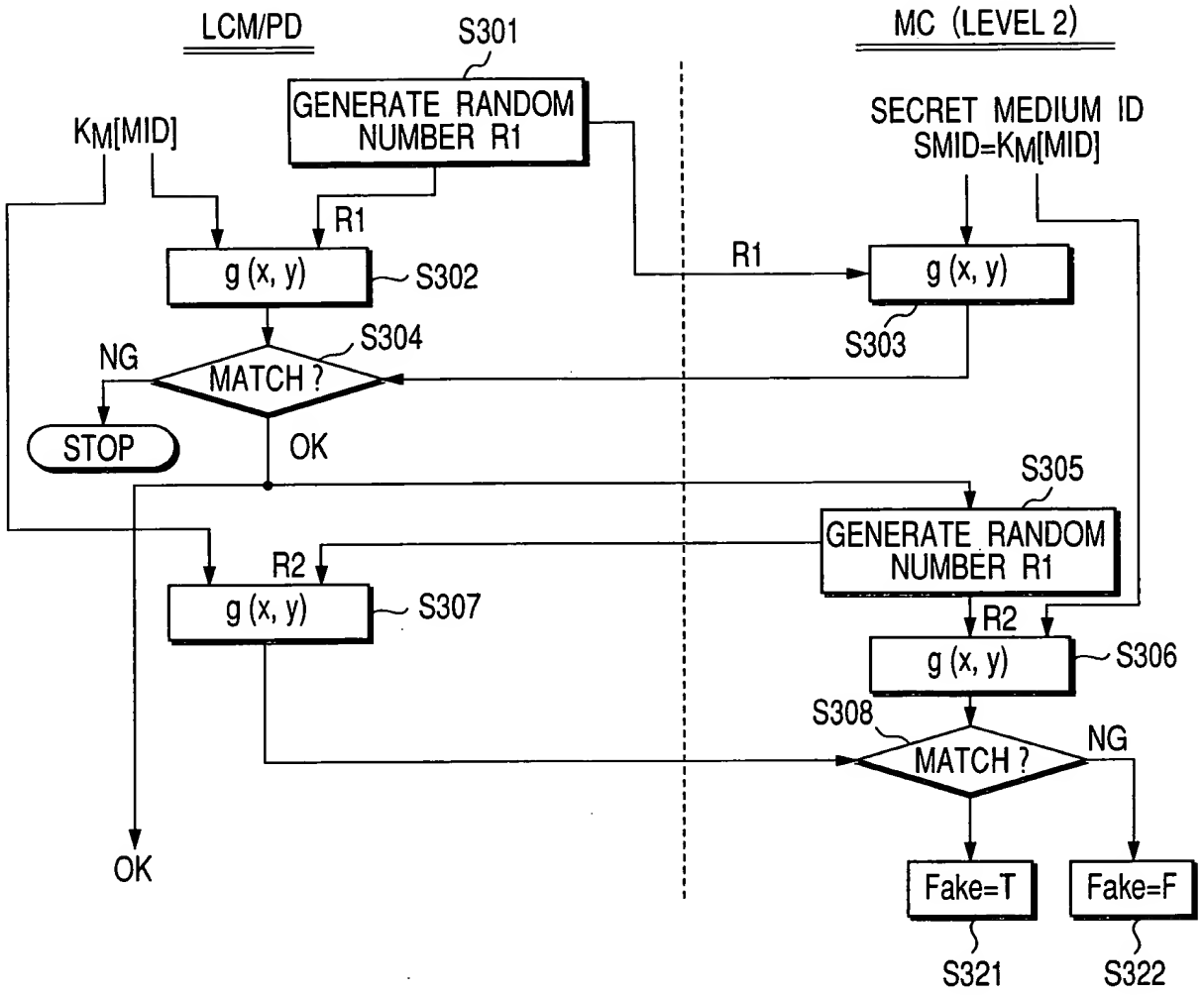
LCM/PD
S301
GENERATE RANDOM NUMBER R1
MC (LEVEL 2)
SECRET MEDIUM ID
SMID=KM[MID]
KM[MID]
R1
g (x, y)
S302
R1
g (x, y)
S303
NG
S304
MATCH ?
STOP
OK
S305
GENERATE RANDOM NUMBER R1
R2
g (x, y)
S307
R2
g (x, y)
S306
S308
MATCH ?
NG
OK
Fake=T
Fake=F
S321
S322

FIG. 22